02C76.2202

United States Senate

COMMITTEE ON
GOVERNMENT OPERATIONS
WASHINGTON, D.C. 20510

August 3, 1976

AT [redacted]

Assistant Legislative Counsel
Central Intelligence Agency
Washington, D.C. 20505

AT Dear [redacted]

This is in connection with the preliminary staff investigation of the Senate Government Operations Committee concerning problems associated with computer technology in federal programs and private industry.

The draft presentation submitted by you July 30, 1976 in preparation for a final presentation to be made a part of the hearing record touches on virtually all of the points which we had discussed earlier. In that regard, the draft is satisfactory. However, there are aspects of the draft which Phil Manuel and I hope can be further developed.

The Committee's hearing record, for example, will be enhanced if it could be established as to which specific legislative acts, directives and other executive orders can be construed to affect computer operations at the Central Intelligence Agency. It would be useful if you would incorporate the specific language from these specific acts, directives and orders into your final statement.

You note in the draft statement that the Agency's computer security program was formalized in 1967. Because the Agency's requirements for computer security are of a high priority, it would be informative if the Committee's hearing record could reflect the manner in which the Agency formalized its computer security program. Independent inquiry by the Committee staff has indicated that those agencies with national security objectives such as yours have been leaders within the executive branch in terms of protecting their automatic data processing systems and related components against compromise and mismanagement. Not all agencies within the executive branch require security standards as strict as yours. However, that is not to say that these other agencies could not benefit from your own experience in formalizing your computer security program.

Moreover, independent inquiry by the Committee staff has demonstrated that there has, to a certain extent, been an absence of a formalized program of computer security in certain agencies. For that reason, a further development in your statement of how it happened and was occassioned that the Agency formalized its computer security program could be of considerable help to those agencies whose computer security procedures could be strengthened.

With respect to personnel security requirements at the CIA, can a felon be cleared to work on any computer-related operation? Does a criminal background disqualify any individual from employment in or access to computer-related operations at CIA? If so, why? These questions are asked because the Committee staff in its preliminary inquiry has been unable to determine if there are any government-wide standards for personnel working on computer-related projects, either directly for the government or in a government contractor capacity.

In that connection, it would be informative to know what you mean in your draft statement when you refer to the significant emphasis the CIA places on personnel security in the computer field. Please define in your final statement what qualifies a CIA employee as meeting personnel security requirements or standards.

Independent inquiry by the Committee staff has indicated that the CIA is one of the few agencies in the federal government, if not the only agency, which requires personnel to be cleared at the top secret level to have access to computer systems as well as all other systems and facilities. This requirement, coupled with the need to know limitation, is designed to provide maximum security against compromise. Your mission is unique within the government. That being said, though, does it seem practicable to you that a similar system of clearance and need to know limitations could be imposed in other agencies in connection with computer operations only? In other words, are security precautions applicable throughout the CIA capable of being applied in computer security operations in other federal operations? In turn, is the concept realistic enough to be pursued any further? Or is it your judgement that, owing to differing objectives, procedures and overall work style, there would be little to be gained by an effort to have other agencies emulate yours in the computer security field?

In that same line of thinking, would it be possible, within national security constraints, for you to comment in your final statement on the budgetary consideration of providing computer security? You note in your draft statement for example, that the Agency's unique security discipline has advanced and grown with the advancement and growth of the Agency's computer operations. It would be instructive for the Committee's hearing record to include your own computer managers' observations as to the relative increases over the years in the cost of computer operations as compared to the increased costs of computer security. In summary, has it been your experience that the costs of computer-security go up faster as new systems are applied or is it possible that the newer applications, system, hardware and software may one day enable us to provide improved security at less costs?

Next, the concept of security indoctrination, as cited in your draft statement, holds the potential for application elsewhere in the executive branch. The Committee hearing record would be enhanced if, in general terms, Senators could be briefed in your final statement, on the general procedures you follow when introducing personnel to security considerations concerning computers. In addition, the practice of making this a continuing process may be one that other agencies may wish to give consideration to.

While instructing personnel on computer security safeguards on a continuous basis, the CIA, according to the draft statement, also places the entire computer program itself under continuous scrutiny by a group of computer security officers. Again, within the constraints of national security considerations, is it your view that a team of computer security officers, or a group similar, could be introduced into the work patterns of other federal agencies whose ADP systems, while containing sensitive data, do not require such a strict method of securing information. The point that is worth discussing here can be stated in question form: Does an agency have to assume certain of the CIA's high intensity security characteristics in order to provide adequate security safeguards? Or is it possible to deploy several CIA procedures -- the computer security officers mission, for example -- on a selective basis? As we discussed in a previous meeting, the Agency operates in general on the assumption that not only is there a potential for compromise in any system; it is also likely that an attempt will be made to effect that compromise. Is it an achievable goal -- is it even a desirable goal -- to seek to instill that way of thinking into agencies outside the intelligence and defense communities. That question is, of course, for Senators to address. But your observations on that subject would be most instructive for the

Committee's hearing record.

Independent inquiry by the Committee staff has indicated that very many experts in ADP operations are of the opinion that all computer systems are vulnerable to compromise, assuming the would be violator has sufficient resources. Do you concur in that assertion? Please elaborate on your reply.

It is Mr. Manuel's and my view that the original draft statement, supplemented by additional information requested herein, will satisfy the Committee's request for your cooperation. We look forward to your continued assistance.

Sincerely,

Fred Asselin

Fred Asselin
Investigator